



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Ascom i62 VoWiFi Handsets with Avaya Aura® Communication Manager and Avaya Aura® Session Manager – Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning Ascom's i62 VoWiFi handsets to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps for provisioning Ascom's i62 VoWiFi (i62) handsets to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Ascom's i62 handsets are configured to register with Session Manager and are configured with 9640 SIP endpoint template. The Ascom i62 handsets then behave as third-party SIP extensions on Communication Manager. The handsets are able to make/receive internal and PSTN/external calls, and have full voicemail and other telephony features available on Communication Manager.

2. General Test Approach and Test Results

The interoperability compliance testing evaluates the ability of Ascom i62 VoWiFi handsets to make and receive calls to and from Avaya H.323, Avaya SIP, and PSTN endpoints. Avaya Aura® Messaging was used to allow users leave voicemail messages and to demonstrate Message Waiting Indication and DTMF on the Ascom i62 handsets.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and Ascom i62 VoWiFi handsets did not include use of any specific encryption features as requested by Ascom.

Avaya's formal testing and Declaration of Conformity is provided only on the headsets/Smartphones that carry the Avaya brand or logo. Avaya may conduct testing of non-Avaya headset/handset to determine interoperability with Avaya phones. However, Avaya does not conduct the testing of non-Avaya headsets/Smartphones for: Acoustic Pressure, Safety, Hearing Aid Compliance, EMC regulations, or any other tests to ensure conformity with safety, audio quality, long-term reliability or any regulation requirements. As a result, Avaya makes no representations whether a particular non-Avaya headset will work with Avaya's telephones or with a different generation of the same Avaya telephone.

Since there is no industry standard for handset interfaces, different manufacturers utilize different handset/headset interfaces with their telephones. Therefore, any claim made by a headset vendor that its product is compatible with Avaya telephones does not equate to a guarantee that the headset will provide adequate safety protection or audio quality

2.1. Interoperability Compliance Testing

The compliance testing included the test scenarios shown below. Note that when applicable, all tests were performed with Avaya SIP, Avaya H.323, Ascom i62 and PSTN endpoints.

- Basic Calls
- Media Shuffling
- Session Refresh Timer
- Long Duration Call
- Hold and Long Hold, Retrieve and Brokering (Toggle)
- Feature Access Code dialing with special characters
- Attended and Blind Transfer
- Call Forwarding Unconditional, No Reply and Busy
- Call Waiting
- Call Park/Pickup
- EC500, where Avaya deskphone is the primary phone and i62 handset being the EC500 destination.
- Multi-Device Access (MDA)
- Attended Conference (also local three-way calling)
- Do Not Disturb
- Calling Line Name/Identification
- Codec Support (G.711, G.729, G.722)
- DTMF Support
- Coverage
- Voice Mail, Message Waiting Indication
- Serviceability

2.2. Test Results

The tests were all functional in nature and performance testing was not included. All test cases passed successfully with the following observations/limitations noted below:

1. When using the EC500 (concurrent call) feature, if an i62 handset or an Avaya endpoint answers the call before two rings, the call is dropped. This is due to the “Cellular Voice Mail Detection” field default value seen in “off-pbx-telephone configuration-set” form of Communication Manager. The default value for this field is “timed (seconds): 4” which means that if Communication Manager receives an answer within 4 seconds then it will be considered as the cellular voicemail picking up the call, and so call will be dropped and proceed to do Communication Manager coverage processing instead. The workaround is to answer the call after 2 rings, or change the “Cellular Voice Mail Detection” field value to “none” or decrease “timed” value. Note that changing the “off-pbx-telephone configuration-set” affects all users in the same set, so if cellular users are grouped with i62 handset users, calls may be answered by a cellular user’s voicemail instead of following the coverage criteria in Communication Manager.
2. When an i62 handset is configured as an EC500 destination for an Avaya endpoint, an incoming call to the Avaya endpoint will ring both the Avaya endpoint and the i62 handset. When the call is declined on the i62 handset, the Avaya endpoint continues to ring as per normal design.
3. All compliance testing was done using UDP and TCP (preferred) as the transport protocol.
4. Negotiation of G.722 between endpoints, such as the Ascom i62, requires support for the codec to be configured on Communication Manager.
5. Diversion can be accomplished via Feature Access Code configured in Communication Manager or locally via i62 handset setting. The call forward on busy feature however, can only be accomplished via Communication Manager with 486 BUSY HERE automatically sent to the caller by Communication Manager on behalf of the busy endpoint per design.
6. When an Avaya endpoint or an i62 handset calls another i62 handset, after the called i62 handset declines the call, the display for the i62 calling party shows busy whereas the Avaya calling party receives the busy tone.
7. In the blind transfer scenario involving three i62 handsets, where A is the calling, B is the called and transfer-from and C is the transfer-to parties. The display on the transfer-to party C showed “Redirected x y” where “x” is the extension number of the calling party A and “y” is the name of the transfer-from party B. According to Ascom, transfer-to party C displayed information conveyed by Communication Manager, and “redirected” was displayed because the INVITE included a History-Info header (Ascom ticket: MRS-145).
8. Ascom i62 handset supports third party conference, which is, i62 makes two calls simultaneously and conferences the calls locally.
9. When multiple voice messages are left for an i62 handset, the handset shows the total number of messages as only “1” in the display even though there are multiple messages. This is because there is no counter information sent in the NOTIFY from Avaya Aura® Messaging.

10. For Multi-Device Access (MDA) feature in i62 handset to function, i62 needs to be configured using and registering through Endpoint ID. Also the MWI configuration has to be identical on all i62 handsets that are configured for MDA. Refer to **Section 7.3** for details.
11. Per design, i62 handsets do not have a redial button. User needs to use “Call List” and redial the numbers.
12. When outgoing calls are configured to be restricted for an i62 handset on Communication Manager, the i62 display showed “No Channel Available” when user attempted to make an outbound call.
13. When the Ethernet to uplink Wireless Access Point was disconnected and connected back after 60 secs, it took more than 5 mins for the i62 handsets to re-register and able to make new calls. Expected behavior had been that the Ascom i62 would try to re-register as soon as an outgoing call fails due to no response from Session Manager. In this case, the workaround was to restart the phones and get immediate connectivity. Active calls will stay up until session refresh expires when the link to the Session Manager is down.

2.3. Support

Technical support for the Ascom i62 wireless handsets can be obtained through a local Ascom supplier or Ascom global technical support:

- Email: support@ascom.com
- Help desk: +46 31 559450

3. Reference Configuration

Figure 1 shows the network topology during compliance testing. The Ascom i62 VoWiFi handsets connect to an Ascom approved wireless router which is placed on the LAN. The i62 handsets register with Session Manager in order to be able to make/receive calls with the Avaya H.323 and SIP endpoints on Communication Manager and with the PSTN. The handsets are configured by Ascom Windows Portable Device Manager (WinPDM) using the Ascom DeskTop Programmer DP1.

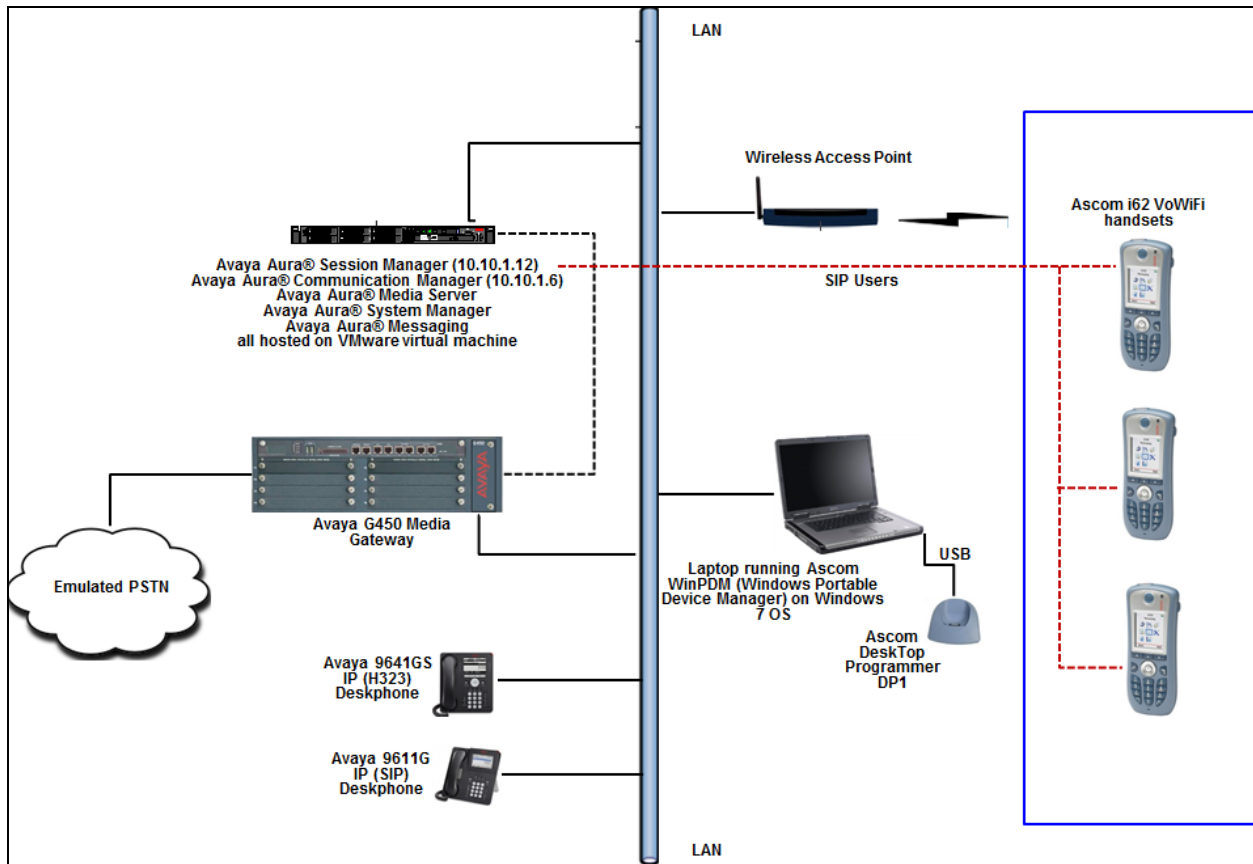


Figure 1: Network Solution of Ascom i62 VoWiFi Handsets with Avaya Aura® Communication Manager and Avaya Aura® Session Manager

4. Equipment and Software Validated

The following equipment and software was used for the compliance test.

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Virtual Server	7.1.2.0.0-FP2
Avaya Aura® Session Manager running on Virtual Server	7.1.2.0.712004
Avaya Aura® System Manager running on Virtual Server	7.1.2.0 (Feature Pack 2)
Avaya Aura® Messaging running on Virtual Server	07.0.0.0.441
Avaya G450 Gateway	38 .18 .0 /1
Avaya IP Deskphones: <ul style="list-style-type: none">• 9641GS (H.323)• 9611G (SIP)	6.6506 7.1.1.0.9
Ascom Windows Portable Device Manager running on Windows 7	3.11.1
Ascom DeskTop Programmer D1	N/A
Ascom i62 VoWiFi handsets	6.0.6

5. Configure Avaya Aura® Communication Manager

It is assumed that a fully functioning Communication Manager is in place with necessary licensing and connecting to Session Manager via SIP Trunk. For further information on the configuration of Communication Manager please see **Section 10** of these Application Notes. The following sections go through the following.

- Dial Plan Analysis
- Feature Access Codes
- Network Region
- IP Codec
- Coverage Path/Hunt Group

Ensure that the SIP endpoints license is valid as shown below by using the command **display system-parameters customer-options**.

display system-parameters customer-options		Page	1 of 12
OPTIONAL FEATURES			
G3 Version: V17	Software Package: Enterprise		
Location: 2	System ID (SID): 1		
Platform: 28	Module ID (MID): 1		
		USED	
Platform Maximum Ports: 48000		168	
Maximum Stations: 36000		44	
Maximum XMOBILE Stations: 36000		0	
Maximum Off-PBX Telephones - EC500: 41000		2	
Maximum Off-PBX Telephones - OPS: 41000		20	
Maximum Off-PBX Telephones - PBFMC: 41000		0	
Maximum Off-PBX Telephones - PVFMC: 41000		0	
Maximum Off-PBX Telephones - SCCAN: 0		0	
Maximum Survivable Processors: 313		1	

Note: A printout of the Signalling and Trunk groups that were used during compliance testing can be found in the **Appendix** of these Application Notes.

5.1. Configure Dial Plan Analysis

Use the **change dialplan analysis** command to configure the dial plan using the parameters shown below. Extension numbers (**ext**) are those beginning with **33** and **34**. Feature Access Codes (**fac**) use digits **8** and **9**. Dial Access Codes (**dac**) use characters ***** or **#**.

change dialplan analysis			DIAL PLAN ANALYSIS TABLE						Page 1 of 12
			Location: all			Percent Full: 5			
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
33	4	ext							
30	4	aar							
33	4	ext							
8	1	fac							
9	1	fac							
*	3	dac							
#	3	dac							

5.2. Configure Feature Access Codes

Use the **change feature-access-codes** command to configure access codes which can be dialed from i62 handsets to initiate Communication Manager call features. These access codes must be compatible with the dial plan described in **Section 5.1**. Some of the access codes configured during compliance testing are shown below.

change feature-access-codes		Page 1 of 10
FEATURE ACCESS CODE (FAC)		
Abbreviated Dialing List1 Access Code:		
Abbreviated Dialing List2 Access Code:		
Abbreviated Dialing List3 Access Code:		
Abbreviated Dial - Prgm Group List Access Code:		
Announcement Access Code: *05		
Answer Back Access Code: 007		
Attendant Access Code:		
Auto Alternate Routing (AAR) Access Code: 8		
Auto Route Selection (ARS) - Access Code 1: 9		Access Code 2:
Automatic Callback Activation:		Deactivation:
Call Forwarding Activation Busy/DA: *07	All: *06	Deactivation: *16
Call Forwarding Enhanced Status:	Act:	Deactivation:
Call Park Access Code: 008		
Call Pickup Access Code: *09		
CAS Remote Hold/Answer Hold-Unhold Access Code: *10		
CDR Account Code Access Code: *11		
Change COR Access Code:		
Change Coverage Access Code:		
Conditional Call Extend Activation:		Deactivation:
Contact Closure	Open Code:	Close Code:

5.3. Configure Network Region

Use the **change ip-network-region x** (where x is the network region to be configured) command to assign an appropriate domain name to be used by Communication Manager, in the example below **bvwdev.com** is used. Note that this domain is also configured in **Section 6.1** of these Application Notes.

```
change ip-network-region 1                                     Page 1 of 20
                                                                IP NETWORK REGION
    Region: 1          NR Group: 1
    Location: 1        Authoritative Domain: bvwdev.com
        Name: Loc-1          Stub Network Region: n
    MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
        Codec Set: 1        Inter-region IP-IP Direct Audio: yes
        UDP Port Min: 2048    IP Audio Hairpinning? n
        UDP Port Max: 3329
    DIFFSERV/TOS PARAMETERS
        Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
    802.1P/Q PARAMETERS
        Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5
    H.323 IP ENDPOINTS    AUDIO RESOURCE RESERVATION PARAMETERS
        H.323 Link Bounce Recovery? y        RSVP Enabled? n
        Idle Traffic Interval (sec): 20
        Keep-Alive Interval (sec): 5
        Keep-Alive Count: 5
```

5.4. Configure IP Codec

Use the **change ip-codec-set x** (where x is the IP codec set used) command to designate a codec set compatible with the i62 handsets. During compliance testing the codecs **G.711MU**, **G.729** and **G.722-64K** were tested.

change ip-codec-set 1

Page 1 of 2

IP MEDIA PARAMETERS

Codec Set: 1

Audio	Silence	Frames	Packet
Codec	Suppression	Per Pkt	Size (ms)
1: G.711MU	n	2	20
2: G.729	n	2	20
3: G.722-64K		2	20
4:			
5:			
6:			
7:			

Media Encryption

Encrypted SRTCP: enforce-unenc-srtcp

1: none

2:

3:

4:

5:

5.5. Configuration of Coverage Path and Hunt Group for Voicemail

The coverage path setup used for compliance testing is illustrated below. Note the following:

Don't Answer is set to **y**: The coverage path will be used in the event the phone set is not answered.

Number of Rings is set to **2**: The coverage path will be used after 2 rings.

Point 1 is set to **h4** Hunt Group 4 is utilised by this coverage path.

```
display coverage path 4

                                COVERAGE PATH

                                Coverage Path Number: 4
                                Cvg Enabled for VDN Route-To Party? n
                                Next Path Number:
                                Hunt after Coverage? n
                                Linkage

COVERAGE CRITERIA
  Station/Group Status   Inside Call   Outside Call
    Active?              n              n
    Busy?                y              y
    Don't Answer?      y              y      Number of Rings: 2
    All?                 n              n
    DND/SAC/Goto Cover?  y              y
    Holiday Coverage?    n              n

COVERAGE POINTS
  Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: h4           Rng:    Point2:
  Point3:                Point4:
  Point5:                Point6:
```

The hunt group used for compliance testing is shown below. Note that on **Page 1** the **Group Extension** is **3333**, which is used to dial for messaging and on **Page 2 Message Center** is set to **sip-adjunct**.

```
display hunt-group 4                                     Page 1 of 60
                                     HUNT GROUP
Group Number: 4                                         ACD? n
Group Name: AMM                                         Queue? n
Group Extension: 3333                                   Vector? n
Group Type: ucd-mia                                     Coverage Path:
TN: 1                                                   Night Service Destination:
COR: 1                                                  MM Early Answer? n
Security Code:                                         Local Agent Preference? n
ISDN/SIP Caller Display:
```

```
display hunt-group 4                                     Page 2 of 60
                                     HUNT GROUP
                                     Message Center: sip-adjunct
Voice Mail Number      Voice Mail Handle      Routing Digits
                                     (e.g., AAR/ARS Access Code)
3000                   3000
```

6. Configure Avaya Aura® Session Manager

The Ascom i62 VoWiFi handsets are added to Session Manager as SIP users. In order make changes in Session Manager a web session to System Manager is opened. Navigate to <http://<System Manager IP address>/SMGR>, enter the appropriate credentials and click on **Log On** as shown below.

Recommended access to System Manager is via FQDN.
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

User ID:

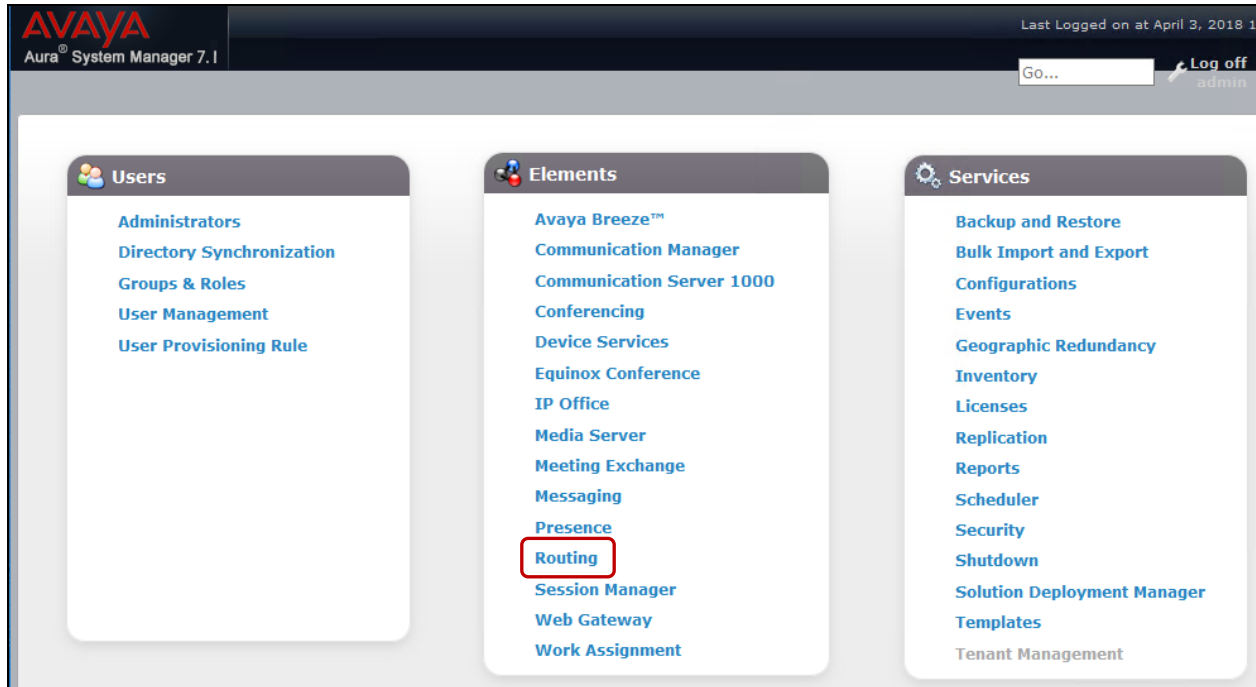
Password:

[Change Password](#)

Supported Browsers: Internet Explorer 11.x or Firefox 48.0, 49.0 and 50.0.

6.1. Configuration of a Domain

Click on **Routing** highlighted below.



Click on **Domains** in the left window. If there is not a domain already configured click on **New** to create a new domain name with **Type sip**. In the example below, there exists a domain called **bvwdev.com** which has been already configured.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The left sidebar has a 'Routing' menu with 'Domains' selected. The main area is titled 'Domain Management' and shows a list of 4 items. The list has columns for Name, Type, and Notes. The domain 'bvwdev.com' is highlighted in blue.

Name	Type	Notes
[Redacted]	sip	
bvwdev.com	sip	SIP Domain
[Redacted]	sip	
[Redacted]	sip	presence domain

Clicking on the domain name above will open the following window; this is simply to show an example of such a domain. When entering a new domain the following should be entered, once the domain name is entered click on **Commit** to save this.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The left sidebar has a 'Routing' menu with 'Domains' selected. The main area is titled 'Domain Management' and shows a single item. The domain 'bvwdev.com' is entered in the Name field, and 'sip' is selected in the Type dropdown. The Notes field contains 'SIP Domain'. The 'Commit' button is visible.

Name	Type	Notes
* bvwdev.com	sip	SIP Domain

6.2. Configuration of a Location

Click on **Locations** in the left window and if there is no location already configured, then click on **New** to create a new location. However, in the screen below, a location called **CM71** is already setup and click into this to show its contents.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The left sidebar contains a tree view with the following items: Routing (selected), Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Location' and shows a list of 11 items. The list has columns for Name, Correlation, and Notes. The item 'CM71' is highlighted in blue. Below the list, there is a 'Select : All, None' option.

<input type="checkbox"/>	Name	Correlation	Notes
<input type="checkbox"/>	[REDACTED]	<input type="checkbox"/>	Aura Messaging Location
<input type="checkbox"/>	[REDACTED]	<input type="checkbox"/>	
<input type="checkbox"/>	[REDACTED]	<input type="checkbox"/>	Simulated as pubic PSTN
<input type="checkbox"/>	[REDACTED]	<input type="checkbox"/>	
<input type="checkbox"/>	[REDACTED]	<input type="checkbox"/>	Cisco Location
<input type="checkbox"/>	CM71	<input type="checkbox"/>	Interop CM 7.1
<input type="checkbox"/>	[REDACTED]	<input type="checkbox"/>	CS1K Car2 Cores
<input type="checkbox"/>	[REDACTED]	<input type="checkbox"/>	Experience Portal 7.1
<input type="checkbox"/>	[REDACTED]	<input type="checkbox"/>	Genesis Location
<input type="checkbox"/>	[REDACTED]	<input type="checkbox"/>	Avaya IP Office SE
<input type="checkbox"/>	[REDACTED]	<input type="checkbox"/>	IP Phone Location

Select : All, None

The Location below shows **Name** with **Location Pattern** of **10.10.1.6**. Once this is configured, click on **Commit**.

AVAYA
Aura® System Manager 7.1

Last Logged on at April 11, 2018 10:10 AM

Go...

Home Routing

Home / Elements / Routing / Locations

Location Details

Commit Cancel

General

* Name: CM71

Notes: Interop CM 7.1

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Location Pattern

Add Remove

1 Item Filter: Enable

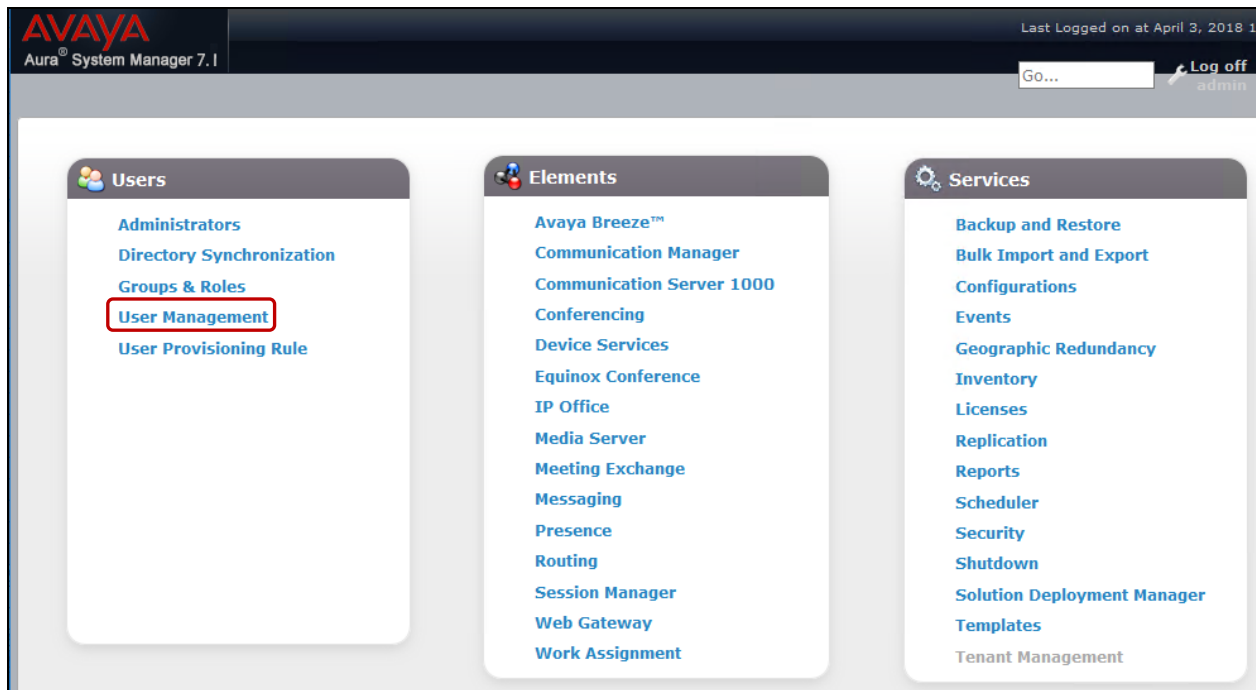
<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.10.1.6	

Select : All, None

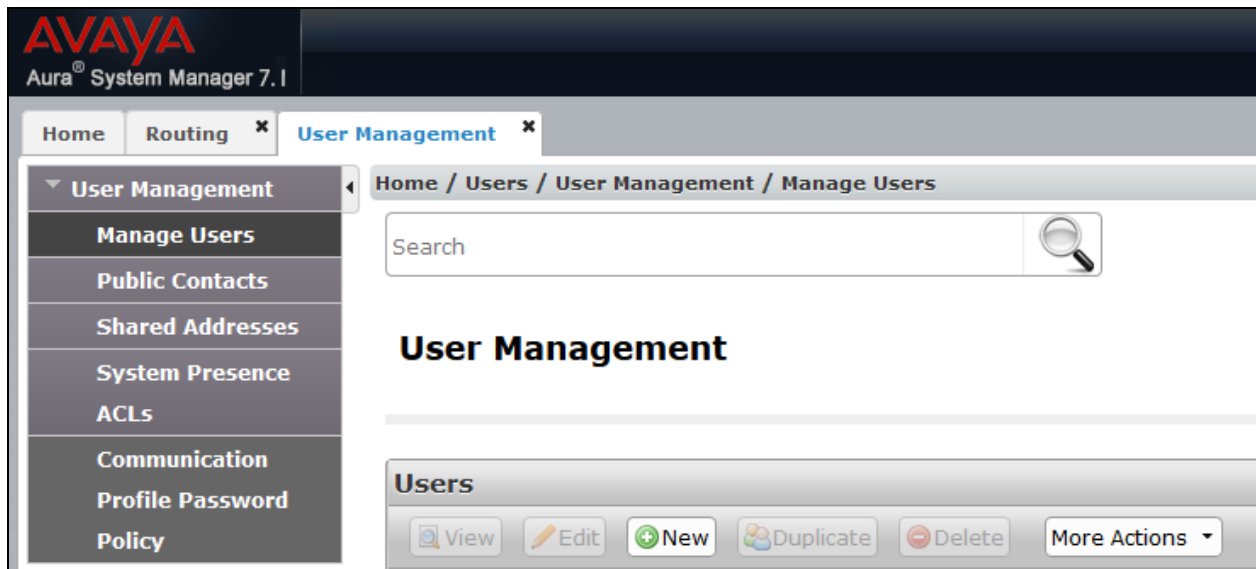
Commit Cancel

6.3. Adding Ascom SIP Users

From the home page click on **User Management** highlighted below.



From **User Management** section, click on **New** to add a new SIP user.



Under the **Identity** tab fill in the user's desired **Last Name** and **First Name** as shown below. Enter the **Login Name** following the format of "user id@domain". The remaining fields can be left as default.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The top navigation bar includes 'Home', 'Routing', and 'User Management'. The left sidebar lists various management options under 'User Management', with 'Manage Users' selected. The main content area is titled 'New User Profile' and contains a 'User Provisioning Rule' dropdown and an 'Identity' section. The 'Identity' section has the following fields:

- * Last Name: 3412
- Last Name (Latin Translation): 3412
- * First Name: Ascom
- First Name (Latin Translation): Ascom
- Middle Name: (empty)
- Description: (empty)
- * Login Name: 3412@bvwddev.com
- Email Address: (empty)
- User Type: Basic

Buttons for 'Commit & Continue', 'Commit', and 'Cancel' are located at the top right of the form. A 'Help' link is also present.

Under the **Communication Profile** tab enter **Communication Profile Password** and **Confirm Password**, note that this password is required when configuring the i62 handset in **Section 7.1**. Click on **New** to add a new **Communication Address**.

The screenshot displays the Avaya Aura System Manager 7.1 web interface. The top navigation bar includes 'Home', 'Routing', and 'User Management'. The left sidebar lists various management options, with 'User Management' expanded. The main content area is titled 'New User Profile' and contains several tabs: 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is currently selected. Within this tab, there are input fields for 'Communication Profile Password' and 'Confirm Password', both masked with dots. A 'Generate' link is positioned to the right of the 'Confirm Password' field. Below these fields, there is a section for 'Communication Address' which includes a 'New' button (highlighted with a red box), an 'Edit' button, and a 'Delete' button. A table with columns 'Type', 'Handle', and 'Domain' is shown below these buttons, indicating 'No Records found'.

AVAYA
Aura® System Manager 7.1

Last Logged on at: [Go...]

Home Routing * User Management *
Home / Users / User Management / Manage Users

Help ?

New User Profile

Commit & Continue Commit Cancel

Identity * Communication Profile Membership Contacts

Communication Profile

Communication Profile Password: [Masked]
Confirm Password: [Masked] [Generate](#)

[New](#) [Delete](#) [Done](#) [Cancel](#)

Name

☒ Primary

Select : None

* Name: Primary

Default : ☒

Communication Address

[New](#) [Edit](#) [Delete](#)

Type	Handle	Domain
No Records found		

Enter the extension number and the domain for the **Fully Qualified Address** and click on **Add** once finished.

Ensure **Session Manager Profile** is checked. Select pertinent values for **Primary Session Manager**, **Origination Application Sequence**, **Termination Application Sequence** and **Home Location** as highlighted below. Note that if this user needs to support MDA feature, then the **Max. Simultaneous Devices** value should be set as required.

Communication Address ▼

New Edit Delete

Type	Handle	Domain
No Records found		

Type: Avaya SIP ▼
* Fully Qualified Address: 3412 @ bvwdev.com ▼
Add Cancel

☒ **Session Manager Profile** ▼

SIP Registration
* Primary Session Manager ASM70A
Secondary Session Manager ASM70A
Survivability Server
Max. Simultaneous Devices 1 ▼
Block New Registration When Maximum Registrations Active? ☐
Application Sequences
Origination Sequence SEQ_InteropCM70 ▼
Termination Sequence SEQ_InteropCM70 ▼
Emergency Calling Application Sequences
Emergency Calling Origination Sequence (None) ▼
Emergency Calling Termination Sequence (None) ▼
Call Routing Settings
* Home Location CM71 ▼

Primary	Secondary	Maximum
23	1	24

Primary	Secondary	Maximum
23	1	24

Ensure that **CM Endpoint Profile** is selected for the **System** and choose the **9640SIP_DEFAULT_CM_7_1** as the **Template**. Click on **Endpoint Editor** to configure the buttons and features for that handset.

☒ **CM Endpoint Profile** ▼

* System interopcm

* Profile Type Endpoint

Use Existing Endpoints ☐

* Extension [Display Extension Ranges](#) 3412 **Endpoint Editor**

* Template 9640SIP_DEFAULT_CM_7_1

Set Type 9640SIP

Under the **General Options** tab ensure that **Coverage Path 1** is set to that configured in **Section 5.5**. Also ensure that **Message Lamp Ext** is showing the correct extension number.

Edit Endpoint

DoneCancel

[Save As Template]

Systeminteropcm

Template9640SIP_DEFAULT_CM_7_1

PortIP

Name3412,Ascom

Extension3412

Set Type9640SIP

Security Code

General Options (G) *Feature Options (F)Site Data (S)Abbreviated Call Dialing (A)

Enhanced Call Fwd (E)Button Assignment (B)Group Membership (M)

* Restriction (COR)1

* Emergency Location Ext3412

* Tenant Number1

* SIP Trunkaar

Coverage Path 14

Lock Message☐

Multibyte LanguageNot Applicable

* Class Of Service (COS)1

* Message Lamp Ext.3412

Type of 3PCC EnabledNone

Coverage Path 2

Localized Display Name3412,Ascom

Enable Reachability for Station Domain Control

Under the tab **Feature Options** ensure that **MWI Served User Type** is set to **sip-adjunct**. Ensure the **Voice Mail Number** is set to that configured in **Section 5.5**.

General Options (G) *		Feature Options (F)		Site Data (S)		Abbreviated Call Dialing (A)	
Enhanced Call Fwd (E)		Button Assignment (B)		Group Membership (M)			
Active Station Ringing	single	Auto Answer	none				
MWI Served User Type	sip-adjunct	Coverage After Forwarding					
Per Station CPN - Send Calling Number	None	Display Language	english				
IP Phone Group ID		Hunt-to Station					
Remote Soft Phone Emergency Calls	as-on-local	Loss Group	19				
LWC Reception	spe	Survivable COR	internal				
AUDIX Name	None	Time of Day Lock Table	None				
Speakerphone	2-way	Voice Mail Number	3333				
Short/Prefixed Registration Allowed	default	Music Source					
EC500 State	enabled						

There must be 3 call appearances setup for the i62 handsets for Call Waiting to work.. Once the **Button Assignment** is completed, click on **Done** (not shown) to finish.

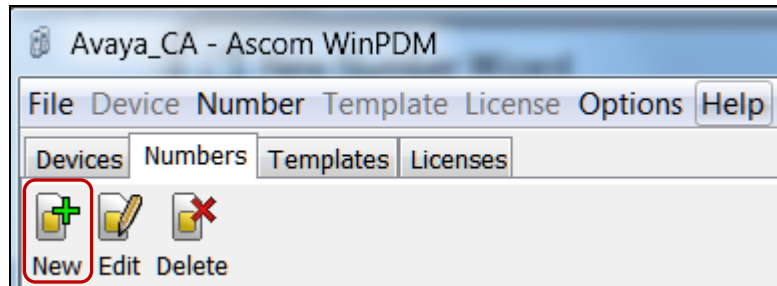
The screenshot shows a web interface for configuring a device. At the top, there are four tabs: 'General Options (G) *', 'Feature Options (F)', 'Site Data (S)', and 'Abbreviated Call Dialing (A)'. Below these, there are three sub-tabs: 'Enhanced Call Fwd (E)', 'Button Assignment (B)', and 'Group Membership (M)'. The 'Button Assignment (B)' tab is currently selected. Under this tab, there are three sub-sections: 'Main Buttons', 'Feature Buttons', and 'Button Modules'. The 'Main Buttons' section contains a table with four rows, each with a number, a dropdown menu, and three empty text input fields. The first three rows have 'call-appr' selected in the dropdown, and the fourth row has 'None' selected.

	Main Buttons	Feature Buttons	Button Modules
1	call-appr ▼	<input type="text"/>	<input type="text"/>
2	call-appr ▼	<input type="text"/>	<input type="text"/>
3	call-appr ▼	<input type="text"/>	<input type="text"/>
4	None ▼	<input type="text"/>	<input type="text"/>

Once the **CM Endpoint Profile** is completed correctly, click on **Commit** (not shown) to save the new user.

7. Configure Ascom i62 VoWiFi Handsets

The configuration of the i62 handsets is done using Ascom's WinPDM software installed on a PC. Attach the Ascom DeskTop Programmer DP1 USB cradle to a PC on which the Ascom WinPDM has been installed. Insert the handset to be configured in the DP1 USB Cradle, start the Ascom Device Manager, select the **Numbers** tab and click **New** icon highlighted below.



Place a new i62 to be programmed into the cradle and the following screen should appear automatically. Select **Edit parameters** and click on **Next** as shown below.



7.1. Configure SIP settings

Select **VoIP → General** from the left window. In the main window ensure the following are set.

- **Replace Call Rejected with User Busy:** **Yes**
- **VoIP Protocol:** **SIP**
- **Codec configuration:** **G.711u-law** (as desired based on **Section 5.4**)
- **Codec packetization time configuration:** **20** (as configured in **Section 5.4**)
- **Internal call number length:** **4** (matches #digits in Endpoint number)
- **Endpoint number:** User extension from **Section 6.3**.
- **Endpoint ID:** Can be left blank

The screenshot shows a configuration window titled "Edit parameters for 3412". At the top, "Device type" is set to "i62 Talker" and "Parameter version" is "14.350". On the left, a tree view shows categories: Network, Device, Audio, Presence, Location, VoIP (expanded), Customization, Headset, User Profiles, and Shortcuts. Under VoIP, "General" is selected. The main area displays a table of parameters:

Name	Value
Replace Call Rejected with User Busy	Yes
ICE negotiation	No
VoIP protocol	SIP
Codec configuration	G.711 u-law
Codec packetization time configuration	20
Offer Secure RTP	No
Internal call number length	4
Endpoint number	3412
Endpoint ID	

Select the **VoIP→SIP** menu point, and enter the values shown below.

- **Primary SIP proxy:** IP address of Session Manager's signaling interface.
- **Listening port:** **5060**
- **SIP proxy password:** Password assigned to the endpoint in **Section 6.3**.
- **Registration identity:** Enter **Endpoint number**.
- **Authentication identity:** Enter **Endpoint number**
- **SIP Register Expiration:** **120** (recommended value)

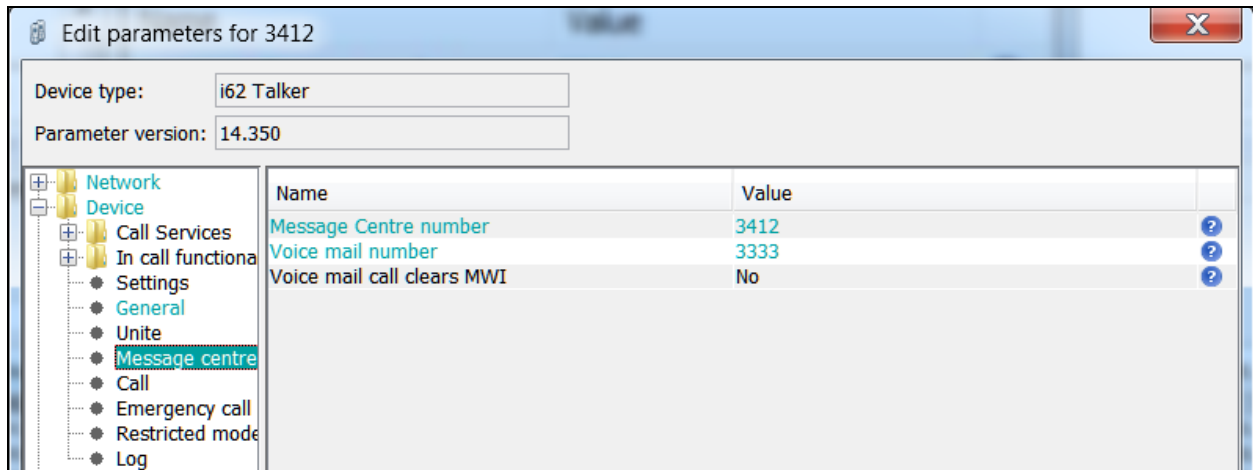
The screenshot shows a window titled "Edit parameters for 3412" with a sidebar on the left containing a tree view of configuration categories: Network, Device, Audio, Presence, Location, VoIP, Customization, Headset, User Profiles, and Shortcuts. Under the VoIP category, there are sub-items: General, H.323, and SIP (which is selected). The main area displays a table of parameters for the selected SIP configuration.

Name	Value
SIP Transport	TCP
Outbound proxy mode	No
Primary SIP proxy	10.10.1.12
Secondary SIP proxy	0.0.0.0
Listening port	5060
SIP proxy ID	
SIP proxy password	*****
Send DTMF using RFC 2833 or SIP INFO	RFC2833
Hold type	Inactive
Registration identity	Endpoint number
Authentication identity	Endpoint number
Call forward locally	Yes
MOH locally	Yes
Hold on Transfer	No
Direct signaling	No
SIP Register Expiration	120
SIP Message behavior	Ignore

For further information about the Ascom i62 handset configurations please refer to Ascom's documentation in **Section 10** of these Application Notes. This section only covers specific settings concerning SIP.

7.2. Configure Message Centre

Click on **Device** → **Message centre** in the left window. In the right window, enter the **Voice mail number** as configured in **Section 5.5** and the **Message Centre number** which is the extension number of the handset.



7.3. Configure Multi-Device Access

The MDA feature allows users to leverage multiple devices (endpoints) simultaneously to meet their communication needs. Users can receive and place calls at multiple devices, and move calls between devices as needed.

For i62 handset, the MDA feature can be accomplished by configuring and registering the handset using the Endpoint ID parameter. In the example below, handset device with extension number 3413 is configured to register as user 3412. As shown in the screen below, **Endpoint number** is configured as **3413** however **Endpoint ID** is configured as **3412**. As per design, the Endpoint number needs to be unique while configuring the i62 handset via WinPDM.

Name	Value
Replace Call Rejected with User Busy	Yes
ICE negotiation	No
VoIP protocol	SIP
Codec configuration	G.711 u-law
Codec packetization time configuration	20
Offer Secure RTP	No
Internal call number length	4
Endpoint number	3413
Endpoint ID	3412

Also the **Registration identity** and **Authentication identity** are both configured as **Endpoint ID** as shown below.

Device type: i62 Talker
Parameter version: 14.350

Name	Value
SIP Transport	TCP
Outbound proxy mode	No
Primary SIP proxy	10.10.1.12
Secondary SIP proxy	0.0.0.0
Listening port	5060
SIP proxy ID	
SIP proxy password	*****
Send DTMF using RFC 2833 or SIP INFO	RFC2833
Hold type	Inactive
Registration identity	Endpoint ID
Authentication identity	Endpoint ID
Call forward locally	Yes
MOH locally	Yes
Hold on Transfer	No
Direct signaling	No
SIP Register Expiration	120
SIP Message behavior	Ignore

For the **Message Centre number** instead of the extension number of the handset, configure the Endpoint ID which is **3412** in this case.

Device type: i62 Talker
Parameter version: 14.350

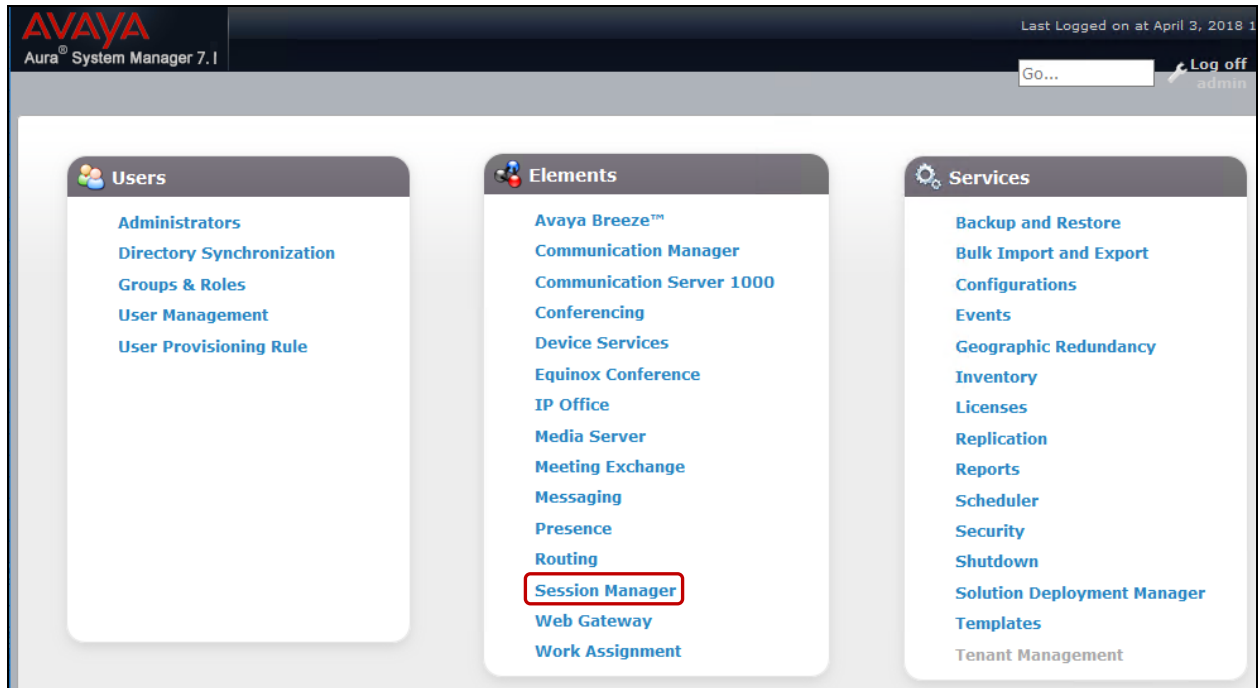
Name	Value
Message Centre number	3412
Voice mail number	3333
Voice mail call clears MWI	No

8. Verification Steps

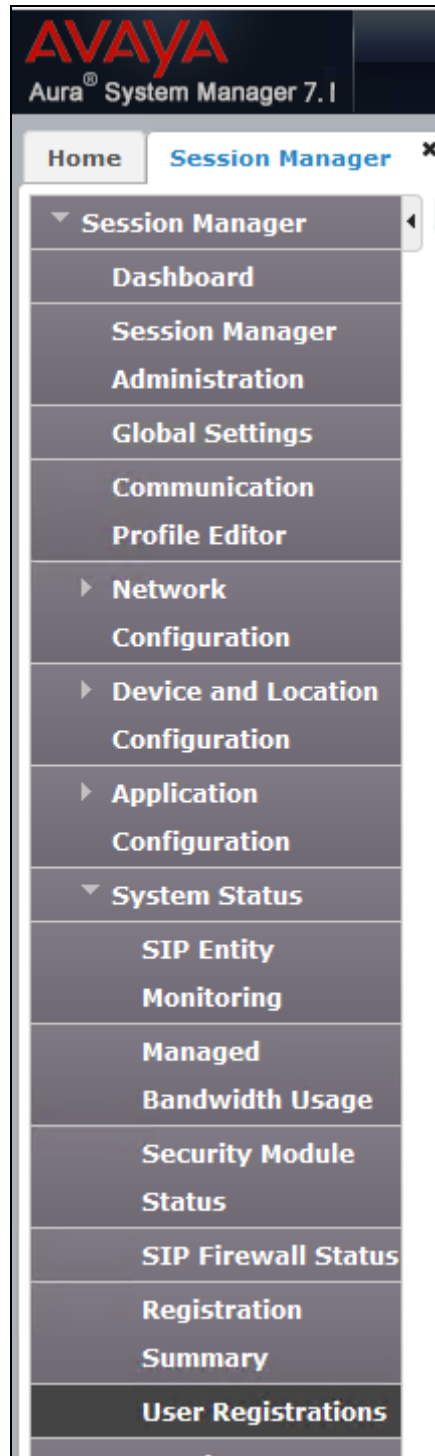
The following steps can be taken to ensure that connections between Ascom i62 handsets and Session Manager and Communication Manager are up.

8.1. Session Manager Registration

Log into System Manager as done previously in **Section 6**, select **Session Manager** as highlighted below.



Under **System Status** in the left window, select **User Registrations** to display all the SIP users that are currently registered with Session Manager.



The Ascom i62 user **3412** should show as being registered as seen below.

User Registrations

Select rows to send notifications to devices. Click on Details column for complete registration status.

View

Default

Export

Force Unregister

AST Device Notifications:

Reboot

Reload

Failback

As of 12:27 PM

Advanced Search

Customize

22 Items

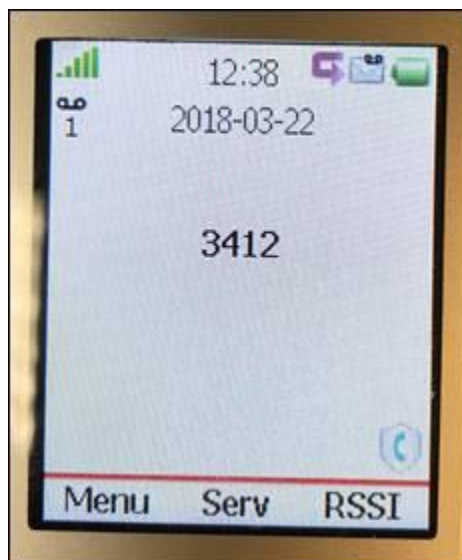
Show 15

Filter: Enable

<input type="checkbox"/>	Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered		
<input type="checkbox"/>											Prim	Sec	Surv
<input type="checkbox"/>	Show	3412@bvwddev.com	Ascom	3412	IP-Phone-Location	---	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

8.2. Ascom i62 Registration

The Ascom i62 handset connection to Session Manager can be verified by an absence of an error message on the handset display just above the red line at the bottom of the display, as shown in the following illustration, (note this is an example from compliance testing).



9. Conclusion

These Application Notes describe the configuration steps required for Ascom's i62 VoWiFi handsets to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager by registering the Ascom i62 handsets with Avaya Aura® Session Manager as SIP users. Please refer to **Section 2.2** for test results and observations.

10. Additional References

This section references the product documentation relevant to these Application Notes.

Product documentation for Avaya products may be found at <http://support.avaya.com>.

1. *Deploying Avaya Aura® Communication Manager*, Release 7.1.2, Issue December 2017
2. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 7.1.2, Issue 4 January 2018
3. *Deploying Avaya Aura® Session Manager*, Release 7.1.2, Issue 4 December 2017
4. *Administering Avaya Aura® Session Manager*, Release 7.1.2, Issue 4 March 2018
5. *Deploying Avaya Aura® System Manager*, Release 7.1.2, Issue 6 March 2018
6. *Administering Avaya Aura® System Manager for Release 7.1.2*, Release 7.1.2, Issue 11 March 2018
7. *Deploying Avaya Aura® Messaging using VMware® in the Virtualized Environment*, Release 7.0.0, Issue 2 January 2017
8. *Administering Avaya Aura® Messaging*, Release 7.0.0, Issue 3 January 2018

Product documentation for Ascom products can be obtained from an Ascom supplier or may be accessed at <https://www.ascom-ws.com/AscomPartnerWeb/Templates/WebLogin.aspx> (login account for the Ascom Partner Extranet required).

Appendix

Signaling Group

display signaling-group 1	SIGNALING GROUP	Page 1 of 2
Group Number: 1	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? n	
Peer Detection Enabled? n	Peer Server: SM	
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr	Far-end Node Name: interopASM	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain: bvwddev.com		
	Bypass If IP Threshold Exceeded? n	
Incoming Dialog Loopbacks: eliminate	RFC 3389 Comfort Noise? n	
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections? y	
Session Establishment Timer(min): 3	IP Audio Hairpinning? n	
Enable Layer 3 Test? y	Initial IP-IP Direct Media? n	
H.323 Station Outgoing Direct Media? n	Alternate Route Timer(sec): 6	

Trunk Group

```
display trunk-group 1                                     Page 1 of 22
                                     TRUNK GROUP

Group Number: 1                Group Type: sip            CDR Reports: y
  Group Name: Private Trunk      COR: 1                TN: 1          TAC: #01
    Direction: two-way          Outgoing Display? n
  Dial Access? n                Night Service:
Queue Length: 0
Service Type: tie                Auth Code? n
                                   Member Assignment Method: auto
                                   Signaling Group: 1
                                   Number of Members: 14
```

```
display trunk-group 1                                     Page 2 of 22
  Group Type: sip

TRUNK PARAMETERS

  Unicode Name: auto

                                   Redirect On OPTIM Failure: 5000

    SCCAN? n                    Digital Loss Group: 18
      Preferred Minimum Session Refresh Interval(sec): 90

Disconnect Supervision - In? y Out? y

    XOIP Treatment: auto        Delay Call Setup When Accessed Via IGAR? n

Caller ID for Service Link Call to H.323 1xC: station-extension
```

```
display trunk-group 1                                     Page 3 of 22
TRUNK FEATURES

  ACA Assignment? n            Measured: none
                                   Maintenance Tests? y

  Suppress # Outpulsing? n      Numbering Format: private
                                   UUI Treatment: shared
                                   Maximum Size of UUI Contents: 128
                                   Replace Restricted Numbers? y
                                   Replace Unavailable Numbers? y
                                   Hold/Unhold Notifications? y
      Modify Tandem Calling Number: no
    Send UCID? y

Show ANSWERED BY on Display? y
```

display trunk-group 1

Page 5 of 22

PROTOCOL VARIATIONS

```

                                Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                                Send Transferring Party Information? n
                                Network Call Redirection? y
Build Refer-To URI of REFER From Contact For NCR? n
                                Send Diversion Header? n
                                Support Request History? y
                                Telephone Event Payload Type:

                                Convert 180 to 183 for Early Media? n
                                Always Use re-INVITE for Display Updates? n
                                Identity for Calling Party Display: P-Asserted-Identity
Block Sending Calling Party Location in INVITE? n
                                Accept Redirect to Blank User Destination? n
                                Enable Q-SIP? n

Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
                                Request URI Contents: may-have-extra-digits
```

©2018 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.